日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　９月３０日

出願番号
Application Number: 特願２００２－２８７７５８

[ST.10/C]: [ＪＰ２００２－２８７７５８]

出願人
Applicant(s): インターナショナル・ビジネス・マシーンズ・コーポレーション

２００３年　２月　７日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３００５３６１

【書類名】　特許願

【整理番号】　JP9020149

【提出日】　平成14年 9月30日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 12/24

H04L 12/26

G06F 13/00

H04L 12/56

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　江藤　博明

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　依田　邦和

【特許出願人】

【識別番号】　390009531

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【代理人】

【識別番号】　100108501

【弁理士】

【氏名又は名称】　上野　剛史

【復代理人】

【識別番号】　100104880

【弁理士】

【氏名又は名称】　古部　次郎

【手数料の表示】

【予納台帳番号】　081504

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9706050

【包括委任状番号】　9704733

【包括委任状番号】　0207860

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信監視システム及びその方法、情報処理方法並びにプログラム

【特許請求の範囲】

【請求項１】　ネットワーク上の任意の地点を流れる通信パケットを入力する通信センサ部と、

前記通信センサ部にて入力された通信パケットにて構成される２つのパケットストリームの外形的な類似度を当該通信パケットの到着に応じて計算する類似度計算部と

を備えることを特徴とする通信監視システム。

【請求項２】　前記類似度計算部は、前記２つのパケットストリームを時間経過における各パケットストリームの通信パケットのデータ量を記述したグラフで表し、各パケットストリームのグラフを交差することなく近づけるように移動した場合に当該２つのグラフで囲まれる領域の大きさに基づいて、当該２つのパケットストリームの類似度を計算することを特徴とする請求項１に記載の通信監視システム。

【請求項３】　前記通信センサ部は、前記類似度計算部により計算された類似度の値に応じて、外部へ所定の通報を行うことを特徴とする請求項１に記載の通信監視システム。

【請求項４】　ネットワーク上の任意の地点を流れる通信パケットを入力するパケット入力手段と、

前記パケット入力手段にて入力された通信パケットにてそれぞれ構成される２つのパケットストリームのマッチングを実時間で実行するマッチング手段と

を備えることを特徴とする通信監視システム。

【請求項５】　前記マッチング手段は、前記２つのパケットストリームを構成する各通信パケットのうち、対応するものどうしの時間的なずれに基づいて、当該２つのパケットストリームの外形的な類似度を判断することを特徴とする請求項４に記載の通信監視システム。

【請求項６】　前記マッチング手段による前記２つのパケットストリームの

外形的な類似度の判断結果に応じて、外部へ所定の通報を行う通報手段をさらに備えることを特徴とする請求項５に記載の通信監視システム。

【請求項７】　コンピュータを用いて、ネットワーク上のデータ通信を監視する通信監視方法であって、

前記ネットワーク上の任意の地点から通信パケットを順次取得し、当該通信パケットが属するパケットストリームに関する情報と共に所定の記憶手段に格納するステップと、

所定の通信パケットを取得した場合に、当該通信パケットの取得時刻から一定の時間以内に取得された他の通信パケットを前記記憶手段から取り出すステップと、

取得した前記通信パケットまでを含む第１のパケットストリームと前記記憶手段から取り出された前記他の通信パケットの属する第２のパケットストリームとの外形的な類似度を判断するステップと、

前記類似度の判断結果に応じて、外部へ所定の通報を行うステップと

を含むことを特徴とする通信監視方法。

【請求項８】　前記パケットストリームの外形的な類似度を判断するステップでは、前記２つのパケットストリームを構成する各通信パケットのうち、対応するものどうしの時間的なずれに基づいて、当該２つのパケットストリームの外形的な類似度を判断することを特徴とする請求項７に記載の通信監視方法。

【請求項９】　前記第１のパケットストリームに対して最も類似すると判断された前記第２のパケットストリームを除く他の前記第２のパケットストリームに対する前記類似度の判断に用いた情報を棄却するステップをさらに含むことを特徴とする請求項７に記載の通信監視方法。

【請求項１０】　ネットワーク上を流れる２つのパケットストリームを比較する情報処理方法であって、

前記ネットワーク上の任意の地点から通信パケットを順次取得し、当該通信パケットが属するパケットストリームに関する情報と共に所定の記憶手段に格納するステップと、

所定の通信パケットを取得した場合に、当該通信パケットの取得時刻から一定

の時間以内に取得された他の通信パケットを前記記憶手段から取り出すステップと、

取得した前記通信パケットまでを含む第１のパケットストリームと前記記憶手段から取り出された前記他の通信パケットの属する第２のパケットストリームとのマッチングを行うステップと

を含むことを特徴とする情報処理方法。

【請求項１１】　前記パケットストリームのマッチングを行うステップは、

前記第１、第２のパケットストリームを時間経過における各パケットストリームの通信パケットのシーケンス番号の増分を表したグラフで表し、各パケットストリームのグラフを交差することなく近づけるように移動した場合に当該２つのグラフで囲まれる領域の大きさに基づいて、当該２つのパケットストリームの類似度を計算するステップを含むことを特徴とする請求項１０に記載の情報処理方法。

【請求項１２】　前記パケットストリームの類似度を計算するステップで、前記２つのグラフで囲まれる領域の時間軸方向の長さに応じて、前記類似度の計算のために用いた情報を棄却することを特徴とする請求項１１に記載の情報処理方法。

【請求項１３】　ネットワークに接続されたコンピュータを制御して、当該ネットワーク上のデータ通信を監視するプログラムであって、

前記ネットワーク上の任意の地点から通信パケットを順次取得し、当該通信パケットが属するパケットストリームに関する情報と共に所定の記憶手段に格納する処理と、

所定の通信パケットを取得した場合に、当該通信パケットの取得時刻から一定の時間以内に取得された他の通信パケットを前記記憶手段から取り出す処理と、

取得した前記通信パケットまでを含む第１のパケットストリームと前記記憶手段から取り出された前記他の通信パケットの属する第２のパケットストリームとの外形的な類似度を計算する処理と、

前記類似度の計算結果に応じて、外部へ所定の通報を行う処理と

を前記コンピュータに実行させることを特徴とするプログラム。

【請求項１４】　前記プログラムによる前記パケットストリームの類似度を計算する処理では、

前記第１、第２のパケットストリームを時間経過における各パケットストリームの通信パケットのシーケンス番号の増分を表したグラフで表し、各パケットストリームのグラフを交差することなく近づけるように移動した場合に当該２つのグラフで囲まれる領域の大きさに基づいて、当該２つのパケットストリームの類似度を計算することを特徴とする請求項１３に記載のプログラム。

【請求項１５】　ネットワークに接続されたコンピュータを制御して、当該ネットワーク上を流れるデータ通信を監視するプログラムであって、

前記ネットワーク上の任意の地点を流れる通信パケットを入力するパケット入力手段と、

前記パケット入力手段にて入力された通信パケットにてそれぞれ構成される２つのパケットストリームのマッチングを実時間で実行するマッチング手段として前記コンピュータを機能させることを特徴とするプログラム。

【請求項１６】　ネットワークに接続されたコンピュータを制御して、当該ネットワーク上を流れるデータ通信を監視するプログラムを格納した記録媒体であって、

前記プログラムは、

前記ネットワーク上の任意の地点から通信パケットを順次取得し、当該通信パケットが属するパケットストリームに関する情報と共に所定の記憶手段に格納する処理と、

所定の通信パケットを取得した場合に、当該通信パケットの取得時刻から一定の時間以内に取得された他の通信パケットを前記記憶手段から取り出す処理と、

取得した前記通信パケットまでを含む第１のパケットストリームと前記記憶手段から取り出された前記他の通信パケットの属する第２のパケットストリームとの外形的な類似度を計算する処理と、

前記類似度の計算結果に応じて、外部へ所定の通報を行う処理と

を前記コンピュータに実行させることを特徴とする記録媒体。

【請求項１７】　ネットワークに接続されたコンピュータを制御して、当該

ネットワーク上を流れるデータ通信を監視するプログラムを格納した記録媒体であって、

前記プログラムは、

前記ネットワーク上の任意の地点を流れる通信パケットを入力するパケット入力手段と、

前記パケット入力手段にて入力された通信パケットにてそれぞれ構成される２つのパケットストリームのマッチングを実時間で実行するマッチング手段として前記コンピュータを機能させることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークにおけるデータ通信を監視する技術に関し、特にネットワークや端末への侵入、攻撃等の検知に利用できる監視技術に関する。

【０００２】

【従来の技術】

インターネットに代表されるコンピュータネットワークでは、所定のネットワークやネットワークに接続された端末に対して正当な権限無く侵入したり攻撃したりする行為（アクセス）を防止するために、セキュリティ手段を設けることが必要となる。

現在、ネットワークのセキュリティ手段としては、ファイア・ウォールが一般的に利用されている。例えば、インターネットとイントラネットの境にファイア・ウォールで構築されたＤＭＺ（De-Militarised Zone：非武装地帯）を通過するＴＣＰコネクションは禁止されている。したがって、ファイア・ウォールのルール設定でインターネットからイントラネットへの直接的な接続は禁止することができる。

また、ネットワークどうしを接続するルータには、通過するデータ通信（以下、単に通信と称す）を制限するためのフィルタ機能があり、これを用いてネットワーク間の不正なアクセスによる侵入を防止することができる。

【０００３】

また従来、ネットワークにおいて不正なアクセスが発見された場合に、当該不正なアクセスを追跡する技術が提案されている。従来のこの種の不正なアクセスの追跡技術には、ネットワークを行き交う通信パケット（以下、単にパケットと称す）のログデータを、そのデータサイズ及び検知時刻と共に、所定の記憶装置（ログボックス）に蓄積しておき、発見された不正なアクセスと蓄積されたログ情報とのマッチングを行うことにより、当該不正なアクセスを追跡するものがある（例えば、特許文献１参照。）。この種の従来の不正なアクセスの追跡技術によれば、当該不正なアクセスの追跡は、通信が行われている時点でリアルタイムに行われるのではなく、蓄積されたログ情報を用いてオフラインで行われている。

【０００４】

【特許文献１】

特開２００１－２１７８３４号公報（第６－８頁）

【０００５】

【発明が解決しようとする課題】

しかし、上記のようにネットワーク上にファイア・ウォールやルータのフィルタ機能といったセキュリティ手段を設けたとしても、かかるセキュリティ手段の管理下に置かれているホストコンピュータを経由した通信による侵入や攻撃を防止することはできなかった。

上述したインターネットとイントラネットとの間にＤＭＺを構築する例では、インターネットとＤＭＺ内のサーバ（ウェブサーバ、ＤＮＳ（Domain Name System）サーバ、メールサーバ等）との間でＴＣＰコネクションを設定し、さらにＤＭＺ内の当該ウェブサーバとイントラネットとの間でＴＣＰコネクションを設定するというように、ＤＭＺを経由したＴＣＰコネクションは、個々のＴＣＰコネクション自体は正当であるので、ファイア・ウォールのルールで禁止することは困難であった。

【０００６】

また、ルータのフィルタ機能にて通信を制限する場合でも、次のような形での侵入をルータのフィルタ設定で防止することはできなかった。すなわち、攻撃者

は、踏み台となるコンピュータに侵入し、そのコンピュータ上のログを消去した後に、他のコンピュータを攻撃する。これにより、客観的には、あたかも踏み台となったコンピュータから攻撃が行われたかのように見える。通常、攻撃者は複数の踏み台を経由して標的となるコンピュータの攻撃を行う。踏み台としてのコンピュータの利用は、そのコンピュータ自体が侵入されなくても起こりうる。例えば、プロキシサーバを中継器として悪用する場合などである。しかし、踏み台となったコンピュータには侵入による実害が無くても、踏み台としてコンピュータが利用されたという事実は、それを管理している組織の信用失墜につながる。

【０００７】

ネットワーク上で発見された不正なアクセスを追跡する従来の技術は、通信ログとのマッチングを行うことによって当該不正なアクセスの追跡を行うため、上記のようなセキュリティ手段の管理下に置かれているホストコンピュータを経由した通信であっても、追跡（逆探知）が可能である。しかし、マッチングの処理をオフラインで行うため、実際に通信が行われている時点でリアルタイムに不正なアクセス等を監視することができなかった。また、不正なアクセスを追跡するためには、不正なアクセスであることが判明している通信ログが必要であった。

【０００８】

そこで、本発明は、ホストコンピュータを経由した通信や直接的な通信を監視できるようにすることを目的とする。

また本発明は、かかる通信の監視により不正なアクセスによる侵入や攻撃を、不正なアクセスであることが判明している通信ログを必要とせず、かつ実時間（リアルタイム）で検出できるようにすることを目的とする。

【０００９】

【課題を解決するための手段】

上記の目的を達成する本発明は、ネットワーク上の任意の地点を流れる通信パケットを入力するパケット入力手段と、入力された通信パケットにてそれぞれ構成される２つのパケットストリームのマッチングを実時間で実行するマッチング手段とを備える通信監視システムとして実現される。

このパケット入力手段は、ネットワークインターフェイスにてネットワークの

所定の地点（通信を監視しようとする地点）に接続された通信センサ部であり、マッチング手段は、この通信センサ部および通信センサ部にて入力された通信パケットにて構成される２つのパケットストリームの外形的な類似度を通信パケットの到着に応じて計算する類似度計算部とを備える通信監視システムとして実現される。

また、この通信監視システムは、マッチング手段による前記２つのパケットストリームの外形的な類似度の判断結果に応じて、オペレータや管理機構等、外部へ所定の通報を行う通報手段をさらに備える。

【００１０】

ここで、２つのパケットストリームの外形的な類似度とは、データの内容を問わず、データ量や個々のパケットの通信間隔の類似度を意味し、２つのパケットストリームを構成する各通信パケットのうち、対応するものどうしの時間的なずれに基づいて判断される。さらに具体的には、この２つのパケットストリームを時間経過における各パケットストリームの通信パケットのデータ量を記述したグラフで表し、各パケットストリームのグラフを交差することなく近づけるように移動した場合に当該２つのグラフで囲まれる領域の大きさに基づいて、当該２つのパケットストリームの類似度を計算することができる。

【００１１】

また、本発明は、コンピュータを用いてネットワーク上のデータ通信を監視する、次のような通信監視方法として実現される。すなわち、この通信監視方法は、ネットワーク上の任意の地点から通信パケットを順次取得し、この通信パケットが属するパケットストリームに関する情報と共に所定の記憶手段に格納するステップと、所定の通信パケットを取得した場合に、この通信パケットの取得時刻から一定の時間以内に取得された他の通信パケットを記憶手段から取り出すステップと、取得した通信パケットまでを含む第１のパケットストリームと記憶手段から取り出された他の通信パケットの属する第２のパケットストリームとの外形的な類似度を判断するステップと、類似度の判断結果に応じて、外部へ所定の通報を行うステップとを含むことを特徴とする。

さらに好ましくは、この通信監視方法は、第１のパケットストリームに対して

最も類似すると判断された第２のパケットストリームを除く他の第２のパケットストリームに対する類似度の判断に用いた情報を棄却するステップをさらに含む。これにより、コンピュータにおけるメモリ使用量や、ＣＰＵの負荷を軽減することができる。

【００１２】

また、本発明は、ネットワーク上を流れる２つのパケットストリームを比較する、次のような情報処理方法として実現される。すなわち、この情報処理方法は、ネットワーク上の任意の地点から通信パケットを順次取得し、この通信パケットが属するパケットストリームに関する情報と共に所定の記憶手段に格納するステップと、所定の通信パケットを取得した場合に、この通信パケットの取得時刻から一定の時間以内に取得された他の通信パケットを記憶手段から取り出すステップと、取得した通信パケットまでを含む第１のパケットストリームと記憶手段から取り出された他の通信パケットの属する第２のパケットストリームとのマッチングを行うステップとを含むことを特徴とする。

さらに好ましくは、この情報処理方法は、パケットストリームの類似度を計算するステップにおいて、２つのグラフで囲まれる領域の時間軸方向の長さが予め設定された特定の範囲にある場合、パケットストリームの類似度の計算のために用いた情報を棄却する。これにより、コンピュータにおけるメモリ使用量や、ＣＰＵの負荷を軽減することができる。

【００１３】

さらにまた、上記の目的を達成する本発明は、コンピュータを制御して上述した通信監視方法や情報処理方法の各ステップに対応する処理を実行させるプログラム、あるいは上述した通信監視システムの機能をコンピュータに実現させるプログラムとして実現することができる。このプログラムは、磁気ディスクや光ディスク、半導体メモリ、その他の記録媒体に格納して配布したり、ネットワークを介して配信したりすることにより、提供することができる。

【００１４】

【発明の実施の形態】

以下、添付図面に示す実施の形態に基づいて、この発明を詳細に説明する。

なお、本実施の形態では、ネットワークにおける通信プロトコルとしてＴＣＰ（Transmission Control Protocol）を用いた場合について説明する。

図１は、本実施の形態による通信監視システムを実現するコンピュータの構成を示す図である。

図１に示すように本実施の形態を実現するコンピュータは、各種の処理を実行するＣＰＵ１０１と、ＣＰＵ１０１を制御するプログラム及びＣＰＵ１０１にて処理されるデータを保持するメモリ１０２と、ネットワークにおいて送受信されるパケットを入力するためのネットワークインターフェイス１０３とを備える。また、コンピュータは磁気ディスク装置１０４を備え、メモリ１０２に保持されているプログラムやデータを適宜磁気ディスク装置１０４へ退避させる。

【００１５】

図２は、図１に示したコンピュータ等で実現される本実施の形態による通信監視システムの機能構成を説明する図である。

図２を参照すると、本実施の形態による通信監視システムは、通信センサ部１０と、パケットデータベース（ＤＢ）２０と、マッチング候補データベース（ＤＢ）３０と、類似度計算部４０と、候補棄却部５０とを備える。これらの構成要素のうち、通信センサ部１０、類似度計算部４０及び候補棄却部５０は、図１のコンピュータにおけるプログラム制御されたＣＰＵ１０１にて実現される。このプログラムは、磁気ディスクや光ディスク、半導体メモリ、その他の記録媒体に格納して配布したり、ネットワークを介して配信したりすることにより提供することができ、図１の例では、磁気ディスク装置１０４に格納され、メモリ１０２に読み込まれてＣＰＵ１０１を制御し、これら構成要素の機能を実現する。また、パケットデータベース２０及びマッチング候補データベース３０は、メモリ１０２及び磁気ディスク装置１０４にて実現される。

【００１６】

図２に示した構成において、通信センサ部１０は、図１のネットワークインターフェイス１０３を介してネットワーク上のパケットを監視しようとする所定の地点（ポイント）に接続して流れるパケットを入力し、パケットデータベース２０に格納する。接続地点の数は任意であるが、通信の監視は、そのうちの２地点

を流れるパケットに関して行う。また、入力パケットがＴＣＰ通信の開始パケットである場合は、後述するマッチング候補を作成してマッチング候補データベース３０に格納する。そして、入力したパケットが不正な侵入や攻撃である可能性がある場合に、外部（オペレータや所定の管理機構等）へ通報する。すなわち、通信センサ部１０は、パケット入力手段、マッチング候補作成手段および通報手段として機能する。通信センサ部１０の動作の詳細については後述する。

【００１７】

パケットデータベース２０は、通信センサ部１０にて取得されたパケットに関する情報（以下、パケット情報）を保管する。パケット情報は、当該パケットの到着時刻、シーケンス番号、パケットストリーム情報である。ここで、パケットストリームとは、１つのＴＣＰ通信における１方向だけのパケットを取り出したものである。また、パケットストリーム情報とは、ＴＣＰコネクションを表す四つ組み＜発信元ＩＰアドレス、送信先ＩＰアドレス、発信元ポート番号、送信先ポート番号＞及びＴＣＰコネクションに対する向き（コネクションと同じ向きのパケットストリームか反対向きのパケットストリームかを表す）である。これらのパケット情報は、取得されたパケット自身及びそのヘッダ情報等から得られる。また、パケットデータベース２０は、データベースへのアクセス機能として、

１．パケットストリーム情報をインデックスにして関連するパケットのリストが取り出せる。

２．パケットを時刻順に取り出せる。

という機能を持っている。

【００１８】

マッチング候補データベース３０は、後述するパケットストリームのマッチングに用いるため、マッチング候補を格納する。マッチング候補とは、２つのＴＣＰ通信間の類似度計算（後述）の途中経過を保持するためのデータ構造であり、＜２つのパケットストリーム、マッチングのずれ（シーケンス番号）、類似度＞からなるデータ構造である。すなわち、マッチング候補データベース３０は、

・検査対象のパケットストリーム

・比較用パケットストリーム

・マッチングのずれ情報

・類似度を表す情報（面積、最大長、最小長、これらの詳細は後述）

を情報として持つ。また、マッチング候補データベース３０は、データベースへのアクセス機能として、比較用パケットストリームをインデックスとしてマッチング候補を取り出せるという機能を持っている。

【００１９】

類似度計算部４０は、通信センサ部１０からの指示にしたがって、マッチング候補データベース３０からマッチング候補のパケットストリームを取得して、通信センサ部１０が取得したパケットストリームと比較し、両パケットストリームの外形的な類似度（データの内容を問わず、データ量や個々のパケットの通信間隔の類似度）を計算するマッチング手段である。類似度の概念及びその計算方法の詳細については後述する。

候補棄却部５０は、所定のパケットストリームに対するマッチング候補の数が爆発的に増大するのを避けるため、必要に応じてマッチング候補データベース３０に蓄積されたマッチング候補を消去（棄却）する。

【００２０】

次に、本実施の形態によるネットワーク通信の監視が必要となる具体的な状況を想定して、本実施の形態の動作について説明する。

図８は、ＤＭＺ（非武装地帯）の構成例を示す図である。

図８に示すように、ＤＭＺ８１０は、インターネット８２０側からもイントラネット８３０側からも、ファイア・ウォール８１１、８１２を経由しないと内部のサーバ（ウェブサーバ８１３、ＤＮＳサーバ８１４、メールサーバ８１５）に到達できないように構成されている。このＤＭＺ８１０を介在させることにより、ＨＴＴＰ（Hypertext Transfer Protocol）やＳＭＴＰ（Simple Mail Transfer Protocol）などの必要な通信プロトコル以外は遮断することができる。図８において、ファイア・ウォール８１１にはインターネット８２０からウェブサーバ８１３へアクセスするためのルールが設定されており、ファイア・ウォール８１２にはウェブサーバ８１３からイントラネット８３０へアクセスするためのルールが設定されている。これは、例えば電子メールをインターネット８２０からイ

ントラネット８３０内に配送するためである。

この場合、上記の電子メールの配信経路と同様に、まずインターネット８２０からＤＭＺ８１０内のサーバ（例えば図８に示すようにウェブサーバ８１３）にＴＣＰ通信を行い、次にＤＭＺ８１０内のサーバからイントラネット８３０にＴＣＰ通信を行うような侵入経路（図中の矢印参照）は、上記ファイア・ウォール８１１、８１２のルールに適応しているため、ファイア・ウォール８１１、８１２やその他の侵入検知ツールで検出することは困難である。

【００２１】

また、同様の通信の侵入は、サービスプロバイダ（ＩＳＰ：Internet Service Provider）によって提供されているネットワークを使用するコンピュータが踏み台として利用されている状況でも生じ得る。そして、ルータのフィルタ設定では、かかるコンピュータの踏み台として利用を防ぐことはできない。

【００２２】

これらのような、ネットワーク上のセキュリティ管理のなされたホストコンピュータを中継点として利用する侵入や攻撃を防止するため、本実施の形態を用いて、このような中継地点として利用され得るポイントの通信を監視する。

そのために、図２に示した通信監視システムにおいて、ネットワークインターフェイス１０３を介して通信センサ部１０を所望のポイントに接続する。具体的には、図８に示したＤＭＺ８１０を経由したＴＣＰ通信の監視では、ファイア・ウォール８１１のＤＭＺ８１０側のインターフェイスと、ファイア・ウォール８１２のイントラネット８３０側のインターフェイスとに接続する。また、ホストコンピュータの踏み台としての利用を監視する場合は、ルータのインターネット側の各インターフェイスに接続する。なお、通信センサ部１０は、監視しようとするポイントの数に応じて任意の本数の接続を行うことができるが、検出結果は２つのポイントにおけるパケットストリームの類似度として与えられる。

【００２３】

これら２つのポイントにおいて、僅かな時間間隔を置いて、極めて類似したパケットストリームが送信された（ＴＣＰ通信が行われた）ことを検出した場合に、ネットワークまたはネットワークに接続されたシステムへの侵入が行われた可

能性があると考えることができる。そこで、本実施の形態では、このような場合に警報を発し、オペレータ等に対し必要な措置を講ずるように促す。

【００２４】

ここで、２つのパケットストリームの類似度について説明する。

図３は、通信センサ部１０で観測された２つのパケットストリームを、時刻ごとのシーケンス番号の変化として表した図表である。

ここで、シーケンス番号とは、ＴＣＰ通信でどこまでのデータを送ったのか示すための値である。初期値に乱数を採り、送信したデータ量分だけシーケンス番号を増加させる。図３では、時間経過におけるシーケンス番号の増分（すなわち送信されたデータ量）をグラフ化している。

図３に示すグラフの形状は、当該パケットストリームの外形的な特徴を示していると考えられる。そこで、本実施の形態において２つのパケットストリームの類似度とは、２つのグラフを交差することなく近づけるように移動し、当該２つのグラフで囲まれる、Ｘ軸（時間軸）方向の領域（時間的なずれ）が最小になるとき、その領域をＹ軸の高さ（シーケンス番号にて示される送信されたデータ量）で割ったものと定義する。すなわち、各パケットストリームを構成するパケットのうち、対応するものどうしの時間的なずれに基づいて、当該２つのパケットストリームの類似度が判断されることとなる。このことに基づき、マッチング候補データベース３０に格納されるマッチング候補における類似度を表す情報は、当該２つのパケットストリームを表すグラフによって囲まれる領域の面積の総和、当該領域におけるＸ軸方向の長さの最大長および最小長とする（以下、これら領域の大きさを示すパラメータを単に面積、最大長、最小長と呼ぶ）。

【００２５】

このように２つのパケットストリームの類似度を定義すると、一方の通信が終了するまで類似度は算出されないこととなる。しかし、実時間で２つのパケットストリームのマッチングを取るためには、通信の終了時に負荷が集中することは都合が悪い。そこで本実施の形態では、パケットを受信するたびに少しずつ類似度の候補を計算するという方式を採る。

図４は、かかる本実施の形態によるパケットストリームのマッチング方法を説

明する図である。

上述したように、シーケンス番号は初期値を乱数としているので、比較が可能となるように、まず、比較用のパケットストリームの開始時に、検索対象となる全てのパケットストリームに対して、マッチングのずれ（シーケンス番号のずれ）を求めておく。そして、得られた検索対照のパケットストリーム、マッチングのずれ情報を含むマッチング候補を作成する。なお、パケットストリームの開始時点であるので、比較用のパケットストリームは最初のパケットのみ、類似度を表す情報は初期値（後述）が登録される。

【００２６】

以下、順次パケットを受信することで発生する比較用パケットストリームの伸びに応じて、個々のマッチング候補の類似度を変更分だけ計算する。変更分の計算とは、グラフの伸びに応じて新たに囲まれた領域の面積、当該領域のＸ軸方向の最大長および最小長の算出である。各マッチング候補の類似度は、次の計算式で求められる。この方式によれば、グラフの伸び分だけを対象にして計算できるため、計算負荷を分散できる。

類似度＝min[|面積－最小長＊高さ|,|面積－最大長＊高さ|]/高さ

【００２７】

ところで、通信監視システムにおける処理時間およびメモリ使用量は、マッチング候補の数に比例する。マッチング候補の数は、

Ｏ(パケットストリームの数^2＊パケットストリーム中のパケット数)

となることから、実時間処理を行うためには、類似度を計算する過程でマッチング候補を適宜削減することが必須となる。そのために本実施の形態では、２つのＴＣＰ通信の時間差を利用する。

【００２８】

本実施の形態でマッチングを行う２つのＴＣＰ通信の時間差について考えると

、例えば、図８のＤＭＺ８１０内のサーバを経由したインターネットからイントラネット内への通信では、１～２個のホストコンピュータを経由した通信の時間差である。また、ＩＳＰの提供するネットワークを踏み台にした通信では、当該ＩＳＰの管理する小規模なネットワークを経由する時間差である。これらの時間差は、攻撃者の端末上のコマンドレスポンス時間と関係があり、レスポンス時間の半分以下である。以上のことから、マッチングを行う２つのＴＣＰ通信の時間差は１～２秒程度で抑えられると想定される（以下、この時間差を、最大パケット遅延時間と称す）。

したがって、マッチング候補の作成処理において、２つのパケットストリームにおける対応パケットの到着時刻が最大パケット遅延時間以上離れていた場合は、候補を作成しない。また、パケット受信時のマッチング候補の更新において、所定のマッチング候補に関して、図４に示したグラフのＸ軸方向の最大長が最大パケット遅延時間を超えていた場合および最小長が最大パケット遅延時間の符号を負にした値（－最大パケット遅延時間）よりも小さかった場合は、候補棄却部５０によって、当該マッチング候補をマッチング候補データベース３０から消去する。以上の処理により、通信監視システムにおけるメモリ使用量の削減と計算時間の短縮とを実現することができる。

【００２９】

図５は、かかる状況における通信センサ部１０の動作を説明するフローチャートである。

図５に示すように、通信センサ部１０は、まず、ネットワークインターフェイス１０３を介して到着したパケットをパケットデータベース２０に格納する（ステップ５０１）。そして、到着したパケットがパケットストリームの開始パケットであった場合（ＴＣＰ通信の開始であった場合）は、後述の手順にてマッチング候補を作成し、マッチング候補データベース３０に格納する（ステップ５０２、５０３）。

【００３０】

一方、到着したパケットがパケットストリームの開始パケットでない場合は、パケットストリームのマッチングを行う。すなわち、まず当該パケットが含まれ

るパケットストリーム（比較用パケットストリーム）をインデックスとして、マッチング候補データベース３０からマッチング候補を取り出す（ステップ５０２、５０４）。そして、取り出されたマッチング候補のそれぞれに対し、類似度計算部４０により類似度計算処理を実施させる（ステップ５０５）。類似度計算部４０の処理については後述する。

【００３１】

次に、通信センサ部１０は、類似度計算部４０の処理結果に基づき、各マッチング候補の類似度の中で最も小さい値を類似度Ｍとする（ステップ５０６）。そして、比較用パケットストリームのパケット数が予め設定された閾値よりも大きく（すなわち当該比較用パケットストリームが一定以上の長さを持つ）、かつ類似度Ｍが予め設定された閾値よりも小さいとき、通信センサ部１０は、侵入を検出したと判断する（ステップ５０７、５０８）。そして、マッチング候補の情報を警報情報として外部に通報する（ステップ５０９）。

また、ステップ５０６の処理を行った場合に、通信センサ部１０は、候補棄却部５０に指示して、類似度Ｍとした最小の類似度を持ったマッチング候補以外のマッチング候補をマッチング候補データベース３０から消去させる（マッチング候補の削減処理）。

【００３２】

図６は、ステップ５０３のマッチング候補の作成処理を説明するフローチャートである。

図６に示すように、通信センサ部１０は、到着したパケットストリーム開始時のパケット（開始パケット）を比較用のパケットストリームとする（ステップ６０１）。次に、パケットデータベース２０からパケットを新しい順に取り出す（ステップ６０２）。パケットデータベース２０から取り出したパケットと比較用のパケットストリーム（到着したパケット）との時間差が最大パケット遅延時間よりも大きい場合は、処理を終了する（ステップ６０３）。

【００３３】

一方、パケットデータベース２０から取り出したパケットと比較用のパケットストリームとの時間差が最大パケット遅延時間以下である場合は、当該取り出し

たパケットが属しているパケットストリームをパケットデータベース２０から取り出し、検査対象のパケットストリームとする（ステップ６０３、６０４）。そして、当該取り出したパケットの開始シーケンス番号をずれ情報とし（ステップ６０５）、類似度を表す情報の初期値として、面積＝０、最大長＝０、最小長＝∞に設定する（ステップ６０６）。

この後、類似度計算部４０にて類似度計算処理を実施し（ステップ６０７）、ステップ６０２へ戻って、比較用のパケットストリームとの時間差が最大パケット遅延時間以下であるパケットが無くなるまで以上の処理を繰り返す。

【００３４】

以上により、比較用のパケットストリームとの時間差が最大パケット遅延時間以下であるパケットの数分のマッチング候補が作成される。

なお、以上の処理において、比較用のパケットストリーム及び検索対象のパケットストリームに関して、通信センサ部１０がネットワークに接続する２つのポイントのどちらから入力したかを区別していない。また、通信の向きも区別していない。したがって、本実施の形態では、これらの区別無く２つのパケットストリームが得られたならば、マッチングを行い、類似度を計算することとなる。これにより、１つの通信経路を通って所定のネットワークに出入りする攻撃を検出することが可能となる。

【００３５】

図７は、類似度計算部４０による類似度計算処理の動作を説明するフローチャートである。この処理は、通信センサ部１０の指示により（ステップ５０５参照）、図３に示したようなグラフを用いて、比較用パケットストリームが１パケット分だけ伸びるたびに実行される。

まず、追加された１パケットによりグラフが伸びた分で新たに囲われる領域を領域Ｂとし、当該領域Ｂの面積、最大長、最小長、高さを求める（ステップ７０１）。そして、ここまでの２つのパケットストリームの類似度を表す情報（面積、最大長、最小長）を適宜更新する（ステップ７０２）。具体的には、

面積＝直前の面積＋領域Ｂの面積

である。また、直前の最大長よりも領域Ｂの最大長の方が大きいならば、

最大長＝Ｂの最大長

とする。また、直前の最小長よりも領域Ｂの最小長の方が小さいならば、

最小長＝Ｂの最小長

とする。

【００３６】

次に、類似度計算部４０は、これらのパラメータから類似度を計算し、通信センサ部１０に渡す（ステップ７０３）。

また、ステップ７０１で得られた、領域Ｂの最大長が最大パケット遅延時間よりも大きいか、または領域Ｂの最小長が最大パケット遅延時間の符号を負にした値よりも小さい場合は、候補棄却部５０に指示して、当該マッチング候補をマッチング候補データベース３０から消去させる（マッチング候補の削減処理）。

【００３７】

次に、本実施の形態を具体的なネットワークシステムに適用した場合の適用例を説明する。

図９は、複数のネットワーク間の通信において本実施の形態による通信の監視を行う場合の構成例を示す図である。

図９に示すように、複数のネットワーク９１０、９２０、９３０がルータ９０１、９０２を介して接続されているものとする。これを図８と対比すると、ネットワーク９１０がインターネット８２０、ネットワーク９２０がＤＭＺ８１０、ネットワーク９３０がイントラネット８３０、ルータ９０１がファイア・ウォール８１１、ルータ９０２がファイア・ウォール８１２にそれぞれ対応すると想定することができる。また、ホストコンピュータの踏み台としての利用を監視する場合は、ネットワーク９２０内のコンピュータ９２１がホストコンピュータであ

るものと想定することができる。

【００３８】

図９のように構成されたネットワークシステムにおいて、攻撃者は、ネットワーク９１０を通過して、まずネットワーク９２０内のコンピュータ９２１を攻撃する。さらに、コンピュータ９２１のセキュリティホールを攻撃することによって、ネットワーク９３０内のコンピュータ９３１に対する攻撃も成功したものとする。ここで、攻撃者が図９の実線の矢印に示す経路で通信を行ったとすると、この通信に関連するパケットがルータ９０１及びルータ９０２を通過する。

本実施の形態の通信監視システムは、常時、ルータ９０１及びルータ９０２を流れる通信を監視しており、上記の通信を即座に検出する。そして、外部の管理機構に対し、攻撃検出を報告する。

【００３９】

図９に示した例では、本実施の形態により通信を監視するポイントが２箇所であったが、３箇所以上を設定して監視することもできる。この場合は、任意の２箇所の通信の関連性を実時間で検出する。また、特殊な事例として、ネットワーク９１０及びネットワーク９３０が同一のネットワークを構成している場合も有る。その場合、通信センサ部１０が接続されるポイントは１つとなり、本実施の形態は、１つのネットワーク９２０を利用して出入りする攻撃を検出するシステムとして働くこととなる。

【００４０】

なお、上記実施の形態では、ネットワークにおける通信プロトコルとしてＴＣＰを用いることとして説明したが、本実施の形態を適用できる通信プロトコルはＴＣＰに限定されない。ＵＤＰ、その他の通信プロトコルによるネットワーク通信においても適宜、適用することができる。他の通信プロトコルで本実施の形態を用いる場合、各通信プロトコルにおけるパケットの形式に基づいて、パケットデータベース２０を検索するためのパケットストリーム情報や類似度計算に用いるパラメータを設定する。

例えば、通信プロトコルがＵＤＰである場合、パケットストリーム情報は、＜ソースＩＰアドレス、デスティネーションＩＰアドレス、ソースポート、デステ

ィネーションポート＞の四つ組みで分け、各パケットストリームの＜到着時刻、ＵＤＰデータサイズ＞を時刻順に並べたものとなる。また、ＵＤＰを用いる場合、ＴＣＰにおけるシーケンス番号のように、各ストリームに関して所定の時点までに流れたデータの総量（バイト）を計算できる情報がない。そこで、例えばＵＤＰヘッダの中の「ＵＤＰデータサイズ」を利用し、類似判断の際にグラフのＹ軸（縦軸）として用いる送信されたデータの総量を計算して用いる。各ストリームについて所定の時点までに流れたデータの総量は、過去のＵＤＰデータサイズの合計を計算することで求めることができる。

【００４１】

【発明の効果】

以上説明したように、本発明によれば、ホストコンピュータを経由した通信や直接的な通信を監視することが可能となる。

また、本発明によれば、かかる通信の監視により不正なアクセスによる侵入や攻撃を、不正なアクセスであることが判明している通信ログを必要とせず、かつ実時間（リアルタイム）で検出することが可能となる。

【図面の簡単な説明】

【図１】　本実施の形態による通信監視システムを実現するコンピュータの構成を示す図である。

【図２】　図１に示したコンピュータ等で実現される本実施の形態による通信監視システムの機能構成を説明する図である。

【図３】　本実施の形態における通信センサ部で観測された２つのパケットストリームを、時刻ごとのシーケンス番号の変化として表した図表である。

【図４】　本実施の形態によるパケットストリームのマッチング方法を説明する図である。

【図５】　本実施の形態における通信センサ部の動作を説明するフローチャートである。

【図６】　図５におけるステップ５０３のマッチング候補の作成処理を説明するフローチャートである。

【図７】　本実施の形態における類似度計算部による類似度計算処理の動作

を説明するフローチャートである。

【図８】　ＤＭＺ（非武装地帯）の構成例を示す図である。

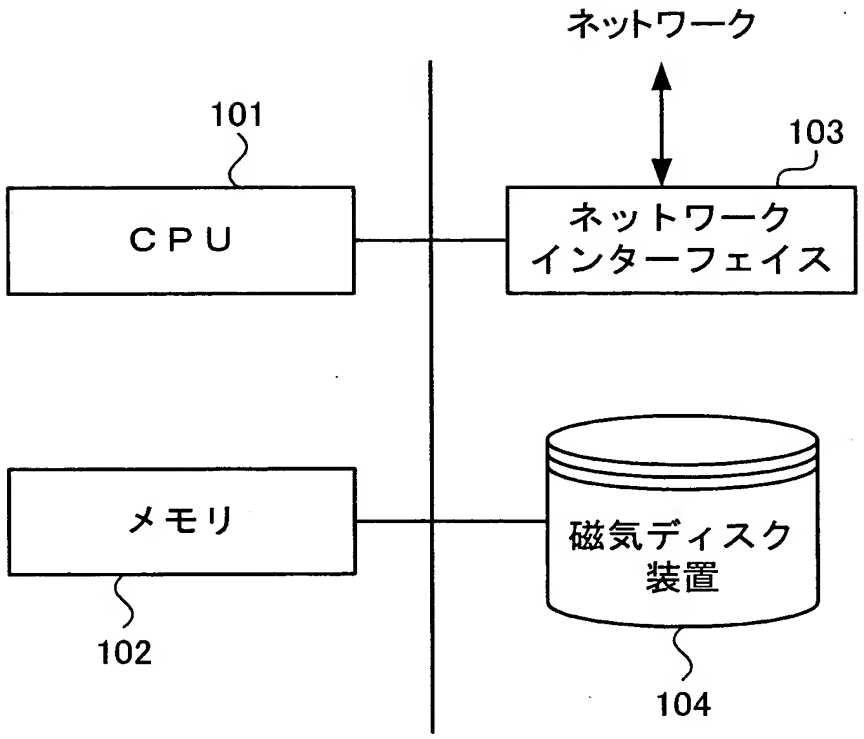
【図９】　複数のネットワーク間の通信において本実施の形態による通信の監視を行う場合の構成例である。

【符号の説明】

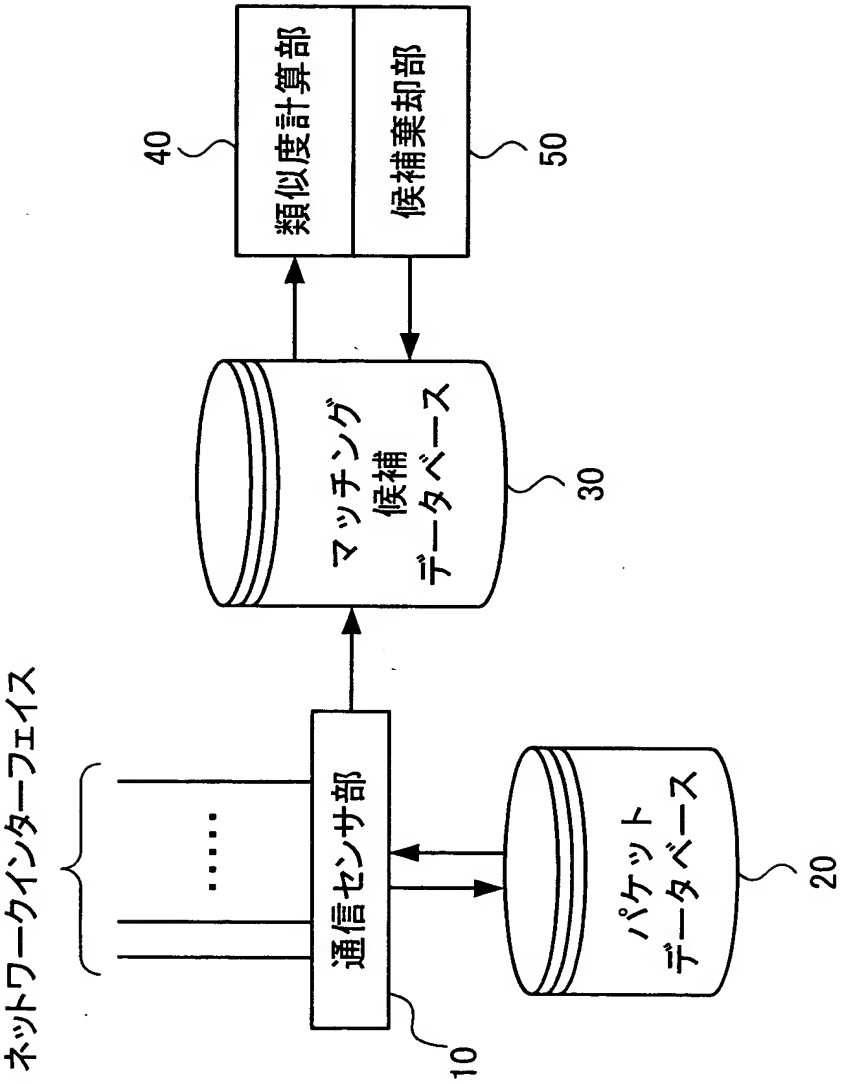
１０…通信センサ部、２０…パケットデータベース（ＤＢ）、３０…マッチング候補データベース（ＤＢ）、４０…類似度計算部、５０…候補棄却部、１０１…ＣＰＵ、１０２…メモリ、１０３…ネットワークインターフェイス、１０４…磁気ディスク装置

【書類名】　　図面

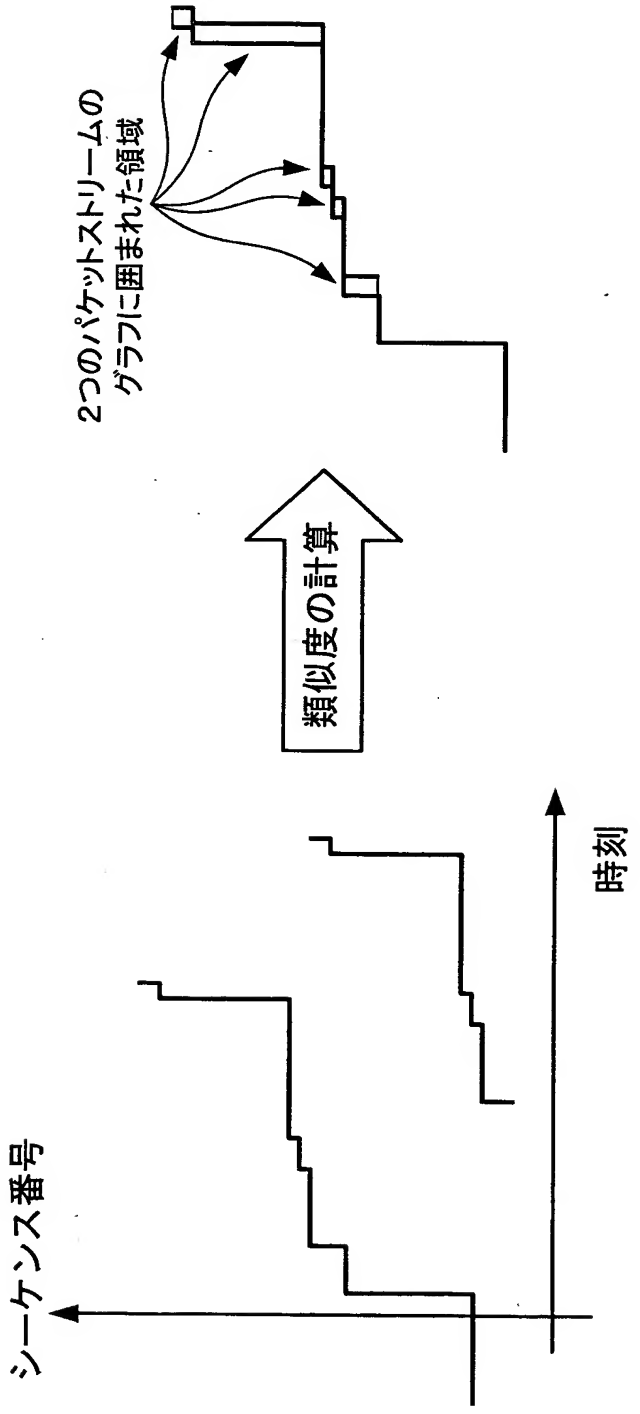
【図１】



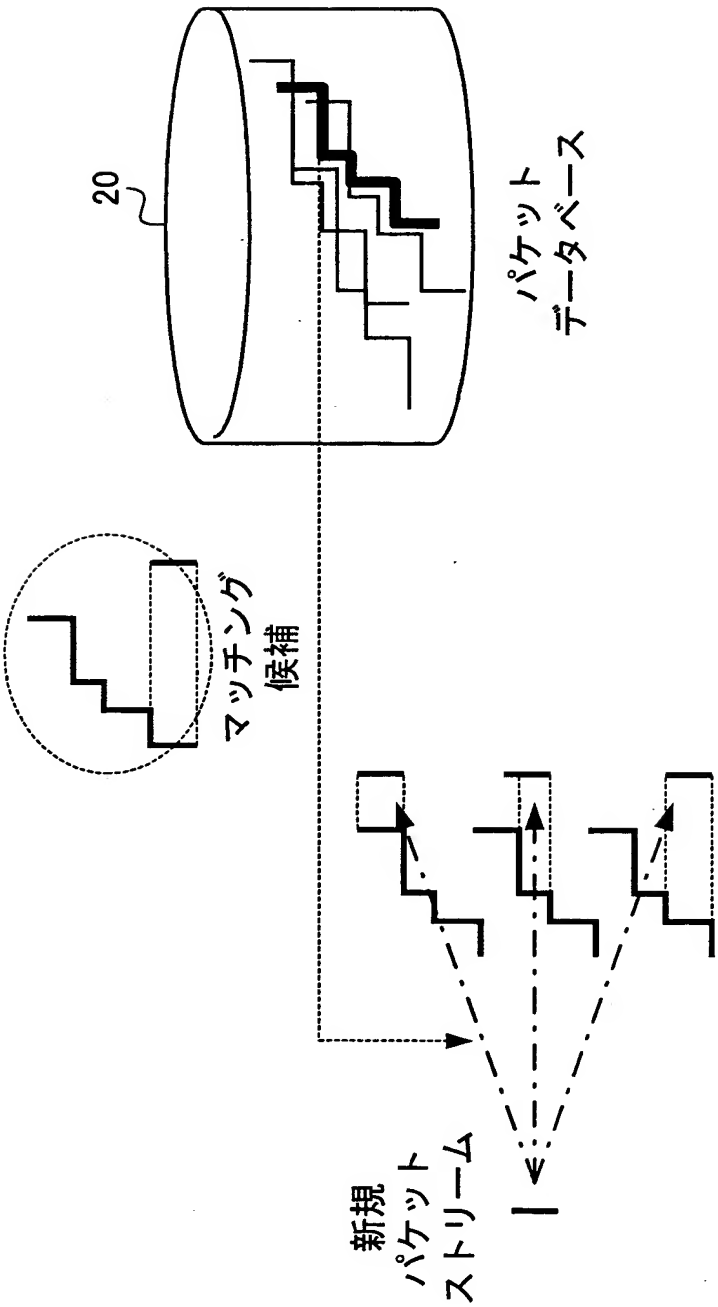
【図２】


類似度計算部
候補棄却部
40
50
マッチング
候補
データベース
30
ネットワークインターフェイス
通信センサ部
10
パケット
データベース
20

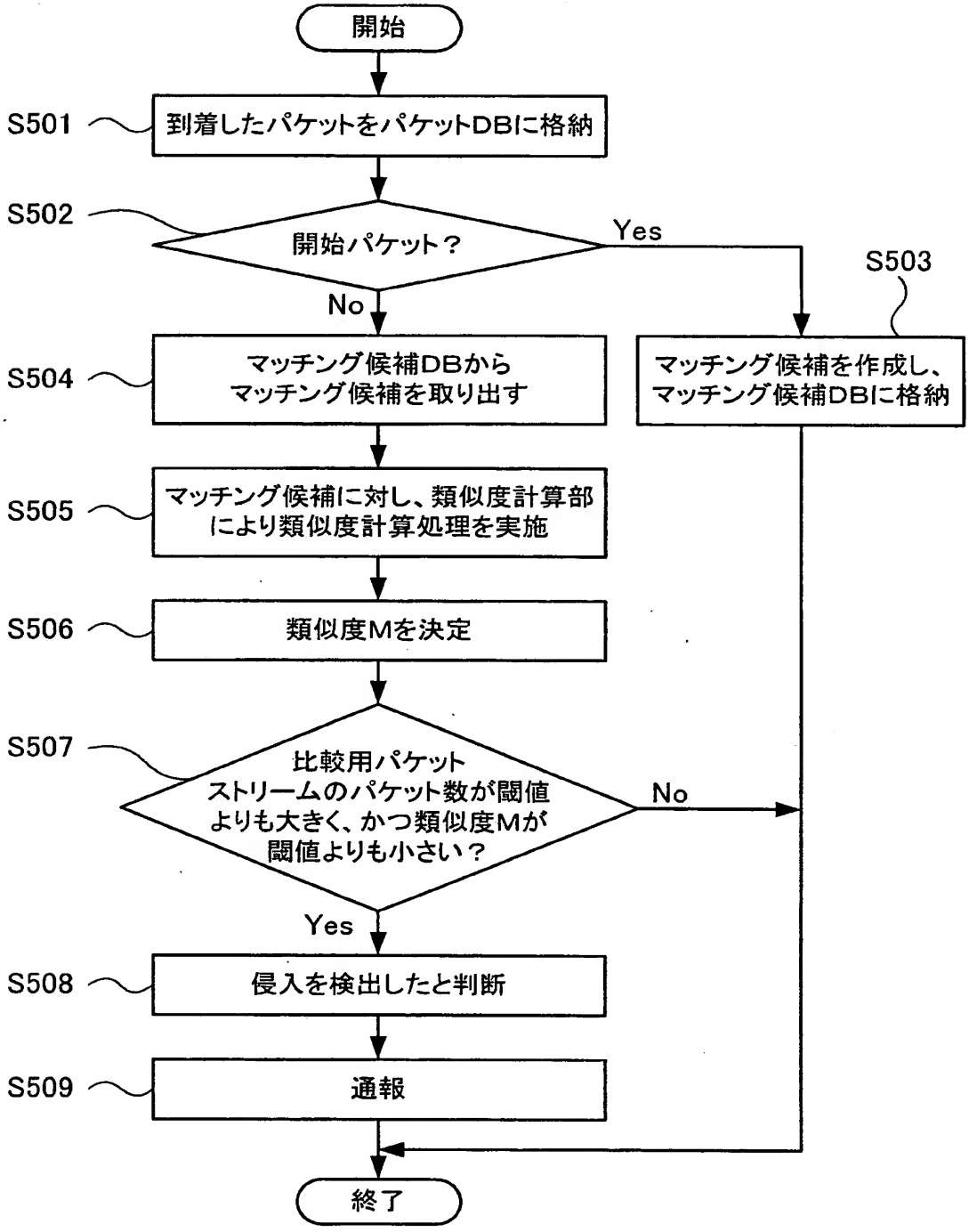
【図３】



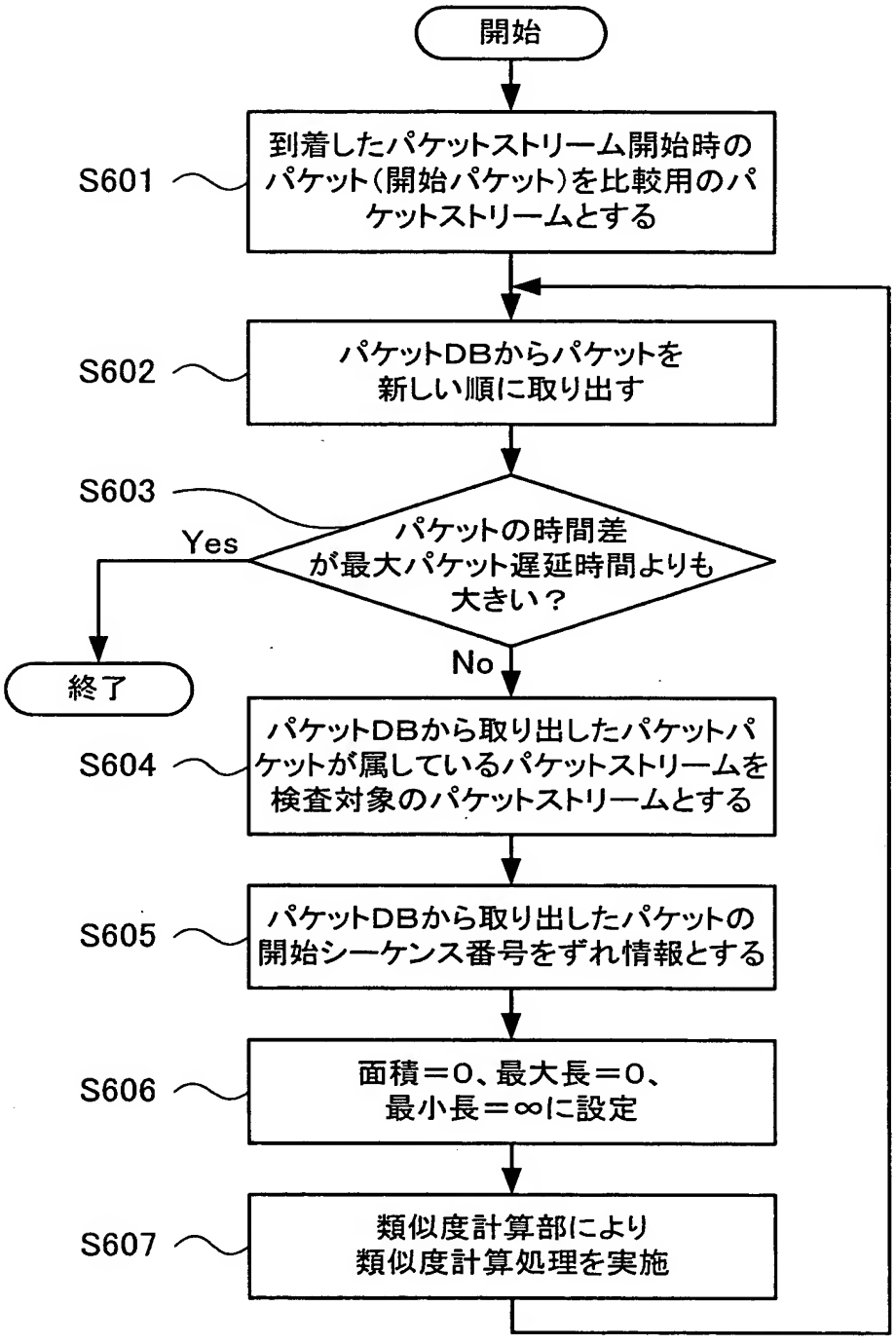
【図４】



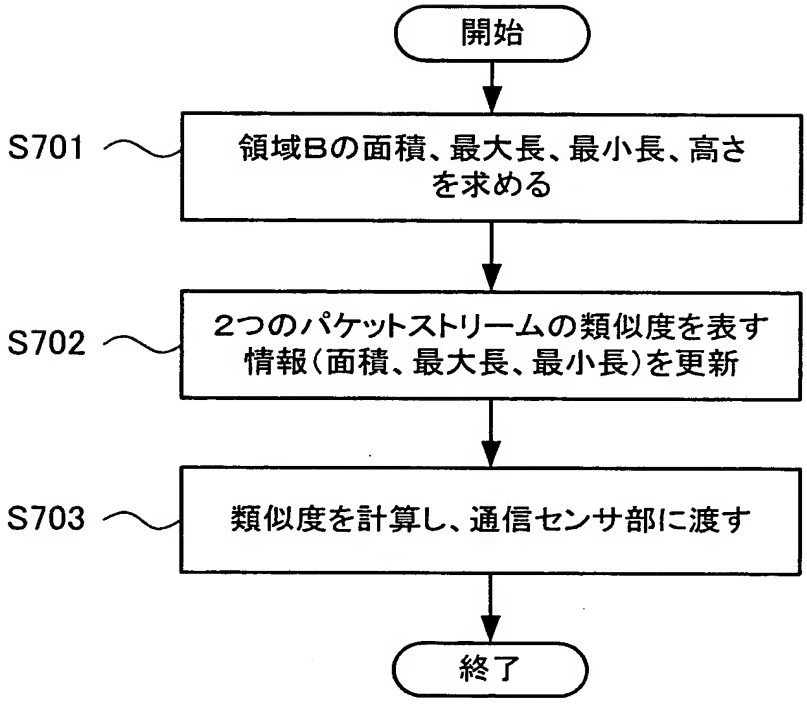
【図５】


開始
S501
到着したパケットをパケットDBに格納
S502
開始パケット？
Yes
No
S503
マッチング候補を作成し、
マッチング候補DBに格納
S504
マッチング候補DBから
マッチング候補を取り出す
S505
マッチング候補に対し、類似度計算部
により類似度計算処理を実施
S506
類似度Mを決定
S507
比較用パケット
ストリームのパケット数が閾値
よりも大きく、かつ類似度Mが
閾値よりも小さい？
No
Yes
S508
侵入を検出したと判断
S509
通報
終了

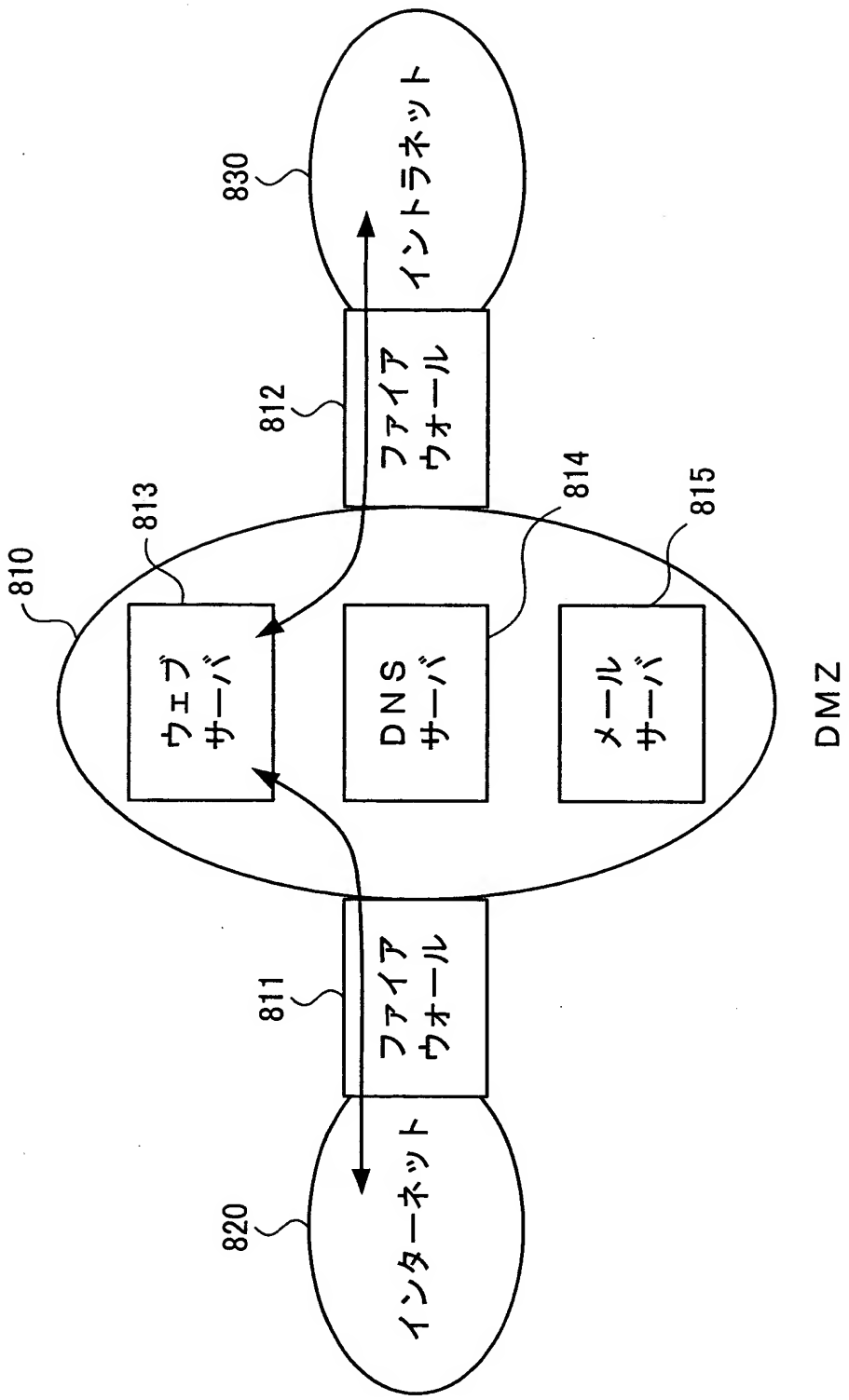
【図６】


開始
S601
到着したパケットストリーム開始時のパケット（開始パケット）を比較用のパケットストリームとする
S602
パケットDBからパケットを新しい順に取り出す
S603
パケットの時間差が最大パケット遅延時間よりも大きい？
Yes
No
終了
S604
パケットDBから取り出したパケットパケットが属しているパケットストリームを検査対象のパケットストリームとする
S605
パケットDBから取り出したパケットの開始シーケンス番号をずれ情報とする
S606
面積＝0、最大長＝0、最小長＝∞に設定
S607
類似度計算部により類似度計算処理を実施

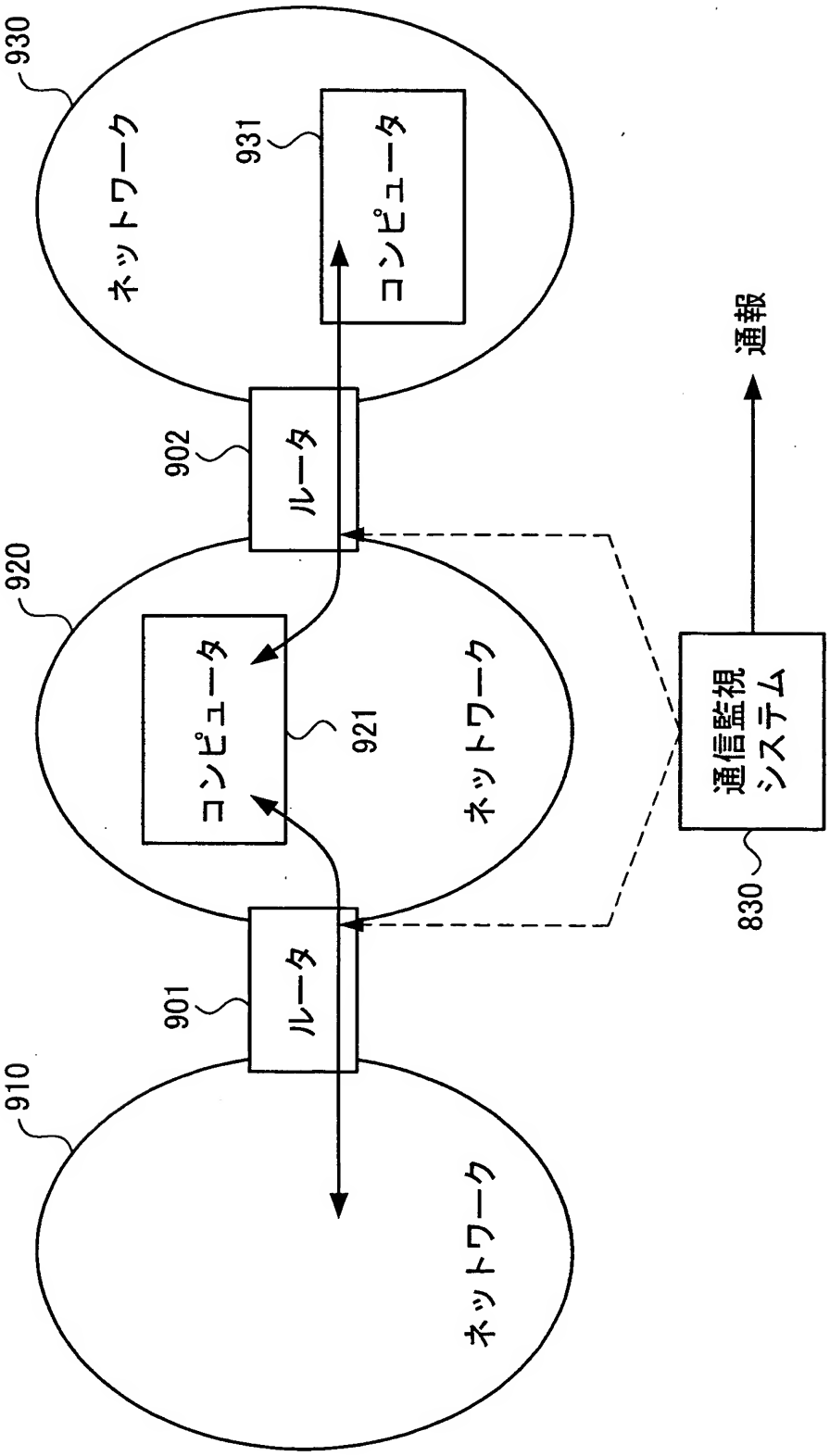
【図７】


開始
S701
領域Bの面積、最大長、最小長、高さを求める
S702
2つのパケットストリームの類似度を表す情報（面積、最大長、最小長）を更新
S703
類似度を計算し、通信センサ部に渡す
終了

【図８】


830
インントラネット
812
ファイア
ウォール
813
814
815
810
ウェブ
サーバ
DNS
サーバ
メール
サーバ
DMZ
811
ファイア
ウォール
820
インターネット

【図９】


930
ネットワーク
931
コンピュータ
902
ルータ
920
コンピュータ
921
ネットワーク
通報
通信監視
システム
830
901
ルータ
910
ネットワーク

【書類名】　　要約書

【要約】

【課題】　ファイア・ウォールやルータのフィルタ機能等のセキュリティ手段の管理下に置かれているホストコンピュータを経由した通信を監視する。

【解決手段】　ネットワークインターフェイスにてネットワークの所定の地点に接続しこの地点を流れる通信パケットを入力するパケット入力手段と、入力された通信パケットにてそれぞれ構成される２つのパケットストリームのマッチングを、通信パケットが入力されるたびに実時間で実行するマッチング手段とを備える。そして、２つのパケットストリームが非常に類似する場合は、侵入や攻撃が行われている可能性が高いと擬制し通報する。

【選択図】　　図２

認定・付加情報

特許出願の番号	特願２００２－２８７７５８
受付番号	５０２０１４７１６４５
書類名	特許願
担当官	井筒　セイ子　　１３５４
作成日	平成１４年１０月　３日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】　390009531

【住所又は居所】　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　市位　嘉宏

【代理人】

【識別番号】　100108501

【住所又は居所】　神奈川県大和市下鶴間１６２３番１４　日本アイ・ビー・エム株式会社　知的所有権

【氏名又は名称】　上野　剛史

【復代理人】　申請人

【識別番号】　100104880

【住所又は居所】　東京都港区赤坂５－４－１１　山口建設第２ビル６Ｆ　セリオ国際特許事務所

【氏名又は名称】　古部　次郎

次頁無

出　願　人　履　歴　情　報

識別番号　　〔３９０００９５３１〕

１．変更年月日　　２００２年　６月　３日
［変更理由］　住所変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション